REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

The Examiner's finding of allowable subject matter at claims 3, 7-9, 17 and 18 is appreciatively noted. No further comment will be made with respect to these allowable claims.

The rejection of claims 1-2, 4-6 and 10-16 under 35 U.S.C. §102 as allegedly being anticipated by the newly cited Watts '627 reference is respectfully traversed.

At the very outset, it is noted that since Watts has nothing whatsoever to do with methods or apparatus for conveying data packets over a packet network from one server to another, etc. it is literally impossible for this reference to anticipate the rejected claims.

Watts literally describes only humanly readable identification cards used in a security system which is to enable the identification of an individual (e.g., when visual contact is not possible or practical). Indeed, Watts explains deficiencies with prior art "smart card" identification systems relying upon the authorized holder to supply a memorized PIN number. It appears that use of the Watts invention is intended to be only where after the identification cards have been distributed to authorized users, a person seeking access is requested to identify themselves and to provide the indicium located at a specified one of the addressable (i.e., row/column) positions on the card that happened to be assigned to that particular identified person. If the indicium matches that assigned to the identified person, then access is granted. Otherwise, access is denied. Optional passwords may also used to help ensure that the person requesting access to a protected premises is actually the authorized person.

It does not appear that the indicium located at particular row/column positions on identification card of Watts are even necessarily machine readable. Clearly there is no teaching or suggestion whatsoever concerning any conveyance of a data packet over a packet network from a first server to another--let alone any of the particular method/apparatus features of applicant's claimed invention.

The claimed invention at issue relates to a method for transmitting data packets in a communications network from a first server to an authorized recipient server. The aim of the invention is to convey the data packet in a way that the authorized recipient server can verify that the received data packet did originate from the genuine first server, and not another third party server.

This done using a two stage process where the first server initially generates a list of random numbers and sends the list securely to the authorized recipient (steps i and ii of claim 1). Then the first server uses one of the random numbers from the generated list and includes it in a data packet and sends that data packet to the authorized first recipient (steps iii and iv of claim 1). The authorized recipient server checks the number in the received data packet to see if it is in the list of numbers originally sent.

Claim 1 thus allows the authorized recipient server to verify that the first server is genuine (e.g., see specification at page 10, lines 14-16). Furthermore, by specifying that the first server cannot use a number that has been included in an earlier data packet, a third party would not be able to monitor data packets and re-use numbers previously used to send false data packets to the authorized recipient (e.g., see specification at page 11, lines 25-30 and step iii of claim 1).

In a further embodiment of the applicant's invention as set out in claim 2, the first server can also verify the authorized recipient server. This is done by the authorized recipient server sending an acknowledgement message containing a sequence number (step v of claim 2) indicative of the position in the stored list of random numbers received by the authorized recipient server. As only the first server and the authorized recipient server have access to this list, this is another good way for the first server to check that the recipient server is indeed the authorized one, and not a third party who has intercepted the original data packet and acknowledging with any sequence number (e.g., see specification at page 10, lines 20-26).

Watts relates to a method of authenticating a user based on ID cards, which have numbers (indicium) printed on them, arranged in a matrix. The cards are distributed by a central system to various users, each card being unique (in the sense that no number in any given position in the matrix on one card is the same as another number in the same position on a different card). When a user requires access to the system, the system asks the user for the number at a particular position in the matrix. The number provided by the user is checked against the expected number at that position to validate the user.

Even at a general level, Watts differs significantly from the claimed invention. For example, Watts is proposing a password system for authenticating users, whereas the claimed invention ensures that data packets are transmitted from a genuine source in a packet network (a packet network being a packet telecommunications network rather than some generic network where the "packets" could just be someone speaking down a phone line). The claimed invention thus provides an indication for a recipient that the data being sent in the packet network is from a valid source (e.g., see specification at page 3, lines 17-21). Claim 1 requires that the first server (the server sending out the original list of random numbers) makes a selection from the list of random numbers and includes it in a data packet which is then sent to the authorized recipient server. This is clearly not the case in Watts where the first server merely asks the recipient for the number at a particular position. As discussed above, by using a number from the stored list to attach to a data packet that is sent, the recipient can determine by checking its list whether the sender is genuine. This could not happen in Watts, as only matrix coordinates are sent by the first server, which of course are not unique. One reason behind this fundamental difference is that in Watts, the user is verified by the server, and not the other way round as in the claimed invention. Furthermore, in Watts, there is no mention of not reusing any number previously used as defined in step ii of claim 1 – a feature that helps insure security against a third party that could monitor data packets and simply reuse numbers for sending out its own false packets.

As for claim 2, Watts also fails to disclose the further steps following those already defined in claim1 relating to authentication of the recipient by sending back an acknowledgement message with a sequence number (see discussion above). In Watts, the number at a particular position is sent back, not the position of a number.

Given the fundamental deficiencies of Watts, is not believe necessary at this time to further discuss the additional deficiencies of this reference with respect to claims 4-6 and 10-16. Suffice it to say that, as a matter of law, the Watts reference cannot possibly anticipate the rejected claims.

The Examiner attention is also drawn to new dependent claims 19-21 which are directed to features utilized at the recipient server (e.g., see steps 250-270 at sic in Fig. 2B and/or as described at page 11, lines 14-30 of the specification). These claims are even further distinguished from any possible teaching (or suggestion) of the cited art.

Accordingly, this entire application is now believed to be in allowable condition and a formal Notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: Larry S. Nixon
Larry S. Nixon
Reg. No. 25,640

LSN:ldw
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100